REMARKS

Claims 1-5, 7-9, 12-14, and 23-33 are pending in the present application. Claims 6, 10, 11, and 15-22 are canceled. Claims 23-33 are added. Reconsideration of the claims is respectfully requested.

Amendments were made to the specification to correct errors and to clarify the specification. No new matter has been added by any of the amendments to the specification.

I. 35 U.S.C. § 102, Anticipation

The Office Action rejects claims 1, 2, 10, 11, 14, 17, 18, 20, and 21 under 35 U.S.C. § 102 as being anticipated by *Handel et al.* (US Patent No. 6,195,651). This rejection is respectfully traversed.

As to claims 1, 2, 10, 11, 14, 17, 18, 20, and 21, the Office Action states:

> As per claims 1, 16, 18, 20, and 21, Handel et al teach a method and software for controlling access to protected contents on a server, the method requiring the following components to be present:
>
> a) a server (column 34, line 19)
>
> b) a client (column 7, lines 60-66)
>
> c) a reader (chip card reader) for a mobile security module (chip card)(column 34, lines 59-60)
>
> d) a security module (chip card) having at least one protected area for storing a key (column 34, lines 59-60)
>
> e) a data line for communications between client and server characterized by the following steps (column 7, lines 60-66):
>
> aa) sending to the server of a request to call up protected access contents (column 34, line 35)
>
> bb) sending from the server to the client of an authentication module to be run in the client (column 8, lines 35-57)
>
> cc) execution of an authentication protocol for authenticating the mobile security module and, where appropriate, its holder by means of the authentication module (column 7, lines 60-67 and column 34, lines 54-65)
>
> dd) if the authentication in step cc) was successful, addition to the request in step aa) of a session ID which was generated in the course of the communications between the authentication module and the server (column 34, lines 63-66 and see attached code on column 42, pertaining to Intention List)
>
> ee) sending of the new request to the server application (column 34, lines 63-66)
>
> ff) checking of the session ID in the request to see that it is recorded in the server (column 34, lines 63-66)

gg) processing of the content requested for transmission and searching of the content for further links to other protected-access contents (column 34, line 60-column 35, line 8)

hh) addition of the session ID to the links identified (column 34, line 60-column 35, line 8)

ii) sending of the content modified as in step hh) to the client (column 34, line 60-column 35, line 8).

Office Action, dated December 8, 2003. Applicants respectfully disagrees. *Handel* teaches a system, method, and article of manufacture for a tuned user application experience. A user's interface to a particular application program is modified by obtaining user profile information. Content is parsed and the parsed content is matched to the user profile information. Matches are presented in a format based on information in the user's profile. See *Handel*, Abstract; col. 1, lines 53-61.

In contradistinction, the present invention provides a mechanism for managing controlled access to protected content on a server using a mobile security module. The mobile security module authenticates with an authentication module. A session identifier (ID) is generated responsive to the mobile security module successfully authenticating with the authentication module.

The Office Action alleges that *Handel* teaches adding a session ID to the request if the authentication was successful and cites col. 34, lines 63-66, as allegedly teaching this features. The cited portion of *Handel* states:

> Personal Profile and Services Ubiquity
>
> This system provides one central storage place for a person's profile. This storage place is a server available through the public Internet, accessible by any device that is connected to the Internet and has appropriate access. Because of the ubiquitous accessibility of the profile, numerous access devices can be used to customize services for the user based on his profile. For example, a merchant's web site can use this profile to provide personalized content to the user. A Personal Digital Assistant (PDA) with Internet access can synchronize the person's calendar, email, contact list, task list and notes on the PDA with the version stored in the Internet site. This enables the person to only have to maintain one version of this data in order to have it available whenever it is needed and in whatever formats it is needed.

FIG. 17 presents the detailed logic associated with the many different methods for accessing this centrally stored profile. The profile database 1710 is the central storage place for the users' profile information. The profile gateway server 1720 receives all requests for profile information, whether from the user himself or merchants trying to provide a service to the user. The profile gateway server is responsible for ensuring that information is only given out when the profile owner specifically grants permission. Any device that can access the public Internet 1730 over TCP/IP (a standard network communications protocol) is able to request information from the profile database via intelligent HTTP requests. Consumers will be able to gain access to services from devices such as their televisions 1740, mobile phones, Smart Cards, gas meters, water meters, kitchen appliances, security systems, desktop computers, laptops, pocket organizers, PDAs, and their vehicles, among others. Likewise, merchants 1750 will be able to access those profiles (given permission from the consumer who owns each profile), and will be able to offer customized, personalized services to consumers because of this.

One possible use of the ubiquitous profile is for a hotel chain. A consumer can carry a Smart Card that holds a digital certificate uniquely identifying him. This Smart Card's digital certificate has been issued by the system and it recorded his profile information into the profile database. The consumer brings this card into a hotel chain and checks in. The hotel employee swipes the Smart Card and the consumer enters his Pin number, unlocking the digital certificate. The certificate is sent to the profile gateway server (using a secure transmission protocol) and is authenticated. The hotel is then given access to a certain part of the consumer's profile that he has previously specified. The hotel can then retrieve all of the consumer's billing information as well as preferences for hotel room, etc. The hotel can also access the consumer's movie and dining preferences and offer customized menus for both of them. The hotel can offer to send an email to the consumer's spouse letting him/her know the person checked into the hotel and is safe. All transaction information can be uploaded to the consumer's profile after the hotel checks him in. This will allow partners of the hotel to utilize the information about the consumer that the hotel has gathered (again, given the consumer's permission).

Handel, col. 34, line 16, to col. 35, line 9. Neither the cited portion, nor any other portion of *Handel*, teaches adding a session ID to a request if a mobile security module successfully authenticates with an authentication module, as recited in claim 1. Rather, *Handel* merely teaches granting access to a user's profile at a hotel terminal if a smart card authenticates with the hotel terminal. The Office Action proffers no analysis as to why this is somehow equivalent to adding a session ID to a request if the mobile security module successfully authenticates with an authentication module, as recited in claim 1.

Furthermore, the Office Action alleges that *Handel* teaches checking of the session ID in the request to see that it is recorded in the server and cites the same portion of the reference as allegedly teaching this feature. Neither the cited portion, nor any other portion of *Handel*, mentions checking whether a session ID is recorded in the server, because, as discussed above, *Handel* does not teach or fairly suggest generating a session ID responsive to a mobile security module successfully authenticating with an authentication module.

Still further, the Office Action alleges that Handel teaches processing the content requested for transmission, searching the content for further links to other protected-access content, and adding the session ID to the identified links and cites the same portion reproduced above as teaching these features. Clearly, the cited portion fails to even mention searching for **links to other** protected-access content. The Office Action proffers no analysis as to why the cited portion of *Handel*, or any other portion, teaches the recited features, but rather baldly concludes that the features are somehow taught.

The applied reference fails to teach or suggest each and every claim limitation. Therefore, claim 1 is not anticipated by *Handel*. Since claims 2 and 14 depend from claim 1, the same distinctions between *Handel* and the invention recited in claim 1 apply for these claims. Additionally, claims 2 and 14 recite other additional combinations of features not suggested by the reference.

Therefore, Applicant respectfully requests withdrawal of the rejection of claims 1, 2, and 14 under 35 U.S.C. § 102.

Furthermore, *Handel* does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. *Handel* actually teaches away from the presently claimed invention because it teaches providing unrestricted access to

an operator of a hotel terminal, upon successful authentication with a smart card, without generating a session ID, as opposed to restricting access to protected content using a session ID, as in the presently claimed invention. Absent the Office Action pointing out some teaching or incentive to implement *Handel* to generate a session ID responsive to successful authentication with a mobile security module, one of ordinary skill in the art would not be led to modify *Handel* to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify *Handel* in this manner, the presently claimed invention can be reached only through an improper use of hindsight using Applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

II. 35 U.S.C. § 103, Obviousness

The Office Action rejects claims 3, 4, 7, 8, and 9 under 35 U.S.C. § 103 as being unpatentable over *Handel* in view of *Hopkins* (US Patent No. 5,757,918). This rejection is respectfully traversed.

Claims 3, 4, 7, 8, and 9 depend from claim 1 and are allowable at least for the reasons stated above with respect to claim 1. Additionally, claims 3, 4, 7, 8, and 9 recite other additional combinations of features not suggested by the reference. As stated above, *Handel* fails to teach or fairly suggest adding a session ID to a request if a mobile security module successfully authenticates with an authentication module, checking of the session ID in the request to see that it is recorded in the server, processing the content requested for transmission, searching the content for further links to other protected-access content, and adding the session ID to the identified links, as recited in claim 1.

Hopkins does teach verifying a smart card and the identity of a user of the smart card to gain access to a security device. However, *Hopkins* does not make up for the deficiencies of *Handel*. To the contrary, *Hopkins* actually teaches away from the presently claimed invention because it teaches verifying a user and/or authenticating a smart card in an off-line environment, as opposed to restricting access to protected content using a session ID, as in the presently claimed invention. Absent the Office Action pointing out some teaching or incentive to implement *Hopkins* to generate a session ID responsive to successful authentication with a mobile security module, one of

ordinary skill in the art would not be led to combine *Handel* and *Hopkins* to reach the present invention when the prior art is examined as a whole. Absent some teaching, suggestion, or incentive to combine *Hopkins* with *Handel* in this manner, the presently claimed invention can be reached only through an improper use of hindsight using Applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

Therefore, Applicants respectfully request withdrawal of the rejection of claims 3, 4, 7, 8, and 9 under 35 U.S.C. § 103.

The Office Action rejects claims 5, 12, and 13 under 35 U.S.C. § 103 as being unpatentable over *Handel* in view of *Lin et al.* (US Patent No. 6,052,785). This rejection is respectfully traversed.

Claims 5, 12, and 13 depend from claim 1 and are allowable at least for the reasons stated above with respect to claim 1. Additionally, claims 5, 12, and 13 recite other additional combinations of features not suggested by the reference. *Lin* does generally teach secure socket layer (SSL) security protocol. However, *Lin* does not make up for the deficiencies of *Handel*. As stated above, *Handel* fails to teach or fairly suggest adding a session ID to a request if a mobile security module successfully authenticates with an authentication module, checking of the session ID in the request to see that it is recorded in the server, processing the content requested for transmission, searching the content for further links to other protected-access content, and adding the session ID to the identified links, as recited in claim 1. Merely combining the teachings of *Handel* with general teachings of SSL would not result in the present invention as recited in claims 5, 12, and 13.

Therefore, Applicants respectfully request withdrawal of the rejection of claims 5, 12, and 13 under 35 U.S.C. § 103.

New claims 23-33 recite subject matter addressed above with respect to claims 1-5, 7-9, 12-14 and are allowable for the same reasons. Additionally, new claims 23-33 recite other additional combinations of features not suggested by the reference. For example, claim 23 recites:

> 23. A method, in a client, for controlling access to protected contents, the method comprising:
>
> sending a request for protected content to a server;

receiving an authentication applet and a random number from the server, wherein the random number is generated at the server;

executing the authentication applet;

sending, by the authentication applet, the random number to a mobile security module, wherein the mobile security module includes a cryptographic key and wherein the mobile security module generates a cryptographic signature based on the key and the random number;

receiving, by the authentication applet, the cryptographic signature from the mobile security module;

sending, by the authentication applet, the cryptographic signature to the server; and

responsive to the server authenticating the cryptographic signature, receiving a session identifier from the server.

Handel, *Hopkins*, and *Lin*, taken alone or in combination, fail to teach or suggest a server authenticating with a mobile security module through an authentication applet executing on a client, as recited in claim 23. *Handel* merely teaches a mechanism for granting access to a profile at a terminal if a smart card authenticates with the terminal. *Hopkins* merely teaches off-line authentication between a smart card and a terminal. *Lin* generally teaches SSL security protocol.

Thus, the prior art, when considered as a whole, fails to teach or suggest the features as recited, in combination, in claim 1. Independent claims 27 and 33 recite subject matter addressed above with respect to claim 23 and are allowable for the same reasons. Since claims 24-26 and 28-32 depend from claims 23 and 27, the same distinctions between the applied references and the invention recited in claims 23 and 27 apply for these claims. Additionally, claims 24-26 and 28-32 recite other additional combinations of features not suggested by the reference.

III. Conclusion

It is respectfully urged that the subject application is patentable over the prior art of record and is now in condition for allowance.

The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: March 8, 2004

Respectfully submitted,

Stephen R. Tkacs
Reg. No. 46,430
Carstens, Yee & Cahoon, LLP
P.O. Box 802334
Dallas, TX 75380
(972) 367-2001
Agent for Applicants